(8) Mostre que as possíveis ordens dos elementos de S_7 são 1, 2, 3, 4, 5, 6, 7, 10 e 12.

Mais uma vez, vamos mostrar alguns resultados auxiliares:

(i) Se $\sigma \in S_n$ é um r-ciclo, então σ tem ordem r.

Seja $\sigma \in S_n$ um r-ciclo,

Denotaremos

$$\sigma = (\alpha_0 . \alpha_1 \dots \alpha_{r-1})$$ (começamos do 0 para fazer aritmética modular)

Vamos provar que $\sigma^k(\alpha_j) = \alpha_{(j+k) \bmod r}$, por indução em k.

Base: $(k=1)$

$$\sigma(\alpha_j) = \begin{cases} \alpha_0 & \text{se } j = r-1 \\ \alpha_{j+1} & \text{se } j < r-1 \end{cases} = \alpha_{(j+1) \bmod r}.$$

Suponha que $\sigma^k(\alpha_j) = \alpha_{(j+k) \bmod r}$ para todo $k < m$ (para algum $m > 1$)

Então

$$\sigma^m(\alpha_j) = \sigma^1(\sigma^{m-1}(\alpha_j)) =$$

$$= \sigma^1(\alpha_{(j+m-1) \bmod r})$$ (Pela hip. de indução, pois $m-1 < m$)

$$= \alpha_{(j+m-1+1) \bmod r}$$ (Pela hip. de indução, pois $1 < m$)

$$= \alpha_{(j+m) \bmod r}.$$

O resultado segue pelo princípio da indução.

Com isso, temos que, para $\alpha_j \in \{\alpha_0, \dots, \alpha_{r-1}\}$

$$\sigma^r(\alpha_j) = \alpha_{(j+r) \bmod r} = \alpha_j$$

Portanto σ^r fixa todos os elementos, então $\sigma^r = Id$.

Agora suponha, por absurdo, que a ordem de σ seja k, com $k < r$.

Então teríamos que

$$\sigma^k(\alpha_0) = \alpha_{(0+k) \bmod r} = \alpha_k$$

Como σ^k é uma composição de bijeções, então $\alpha_0 = \alpha_k$, absurdo, pois num r-ciclo todos os r elementos são distintos.

Portanto a ordem de σ é r.

(ii) Se $n \geq 2$, $\sigma \in S_n$, $\sigma \neq Id$,

Então σ pode ser escrito como um produto de ciclos de comprimento ≥ 2 dois a dois disjuntos.

(Provado em aula, dia 14/10)

(iii) Sejam $\sigma \in S_n$ um r-ciclo e $\tau \in S_n$ um s-ciclo, com σ e τ disjuntos

Se $mdc(r,s) = 1$, então ordem de $\sigma\tau = rs$

Como permutações disjuntas comutam, temos que

$$(\sigma\tau)^{rs} = \sigma^{rs}\tau^{rs} = (\sigma^r)^s(\tau^s)^r = Id$$

Seja k a ordem de $\sigma\tau$.

Temos que $k \mid rs$

Além disso

$$Id = Id^r = ((\sigma\tau)^k)^r = (\sigma\tau)^{kr} = \sigma^{kr}\tau^{kr} = \tau^{kr} \Rightarrow s \mid kr,$$

como r e s são coprimos, então $s \mid k$

Analogamente, temos que $r \mid k$.

Portanto $rs \mid k$

Como $k \mid rs$ e $rs \mid k$ então $k = rs$.

Agora podemos juntar as pesas no nosso caso em S_7.

Seja $\sigma \in S_7$, então há 2 possibilidades:

- σ é um r-ciclo (com $r \in \{1, 2, \dots, 7\}$)

  Nesse caso, a ordem de σ é r.

- σ é uma composisão de ciclos disjuntos de comprimento ≥ 2.

  As únicas combinasões possíveis são:

  - $\sigma =$ 2-ciclo $\circ$ 5-ciclo, nesse caso, σ tem ordem $10 = 2 \cdot 5$.

  - $\sigma =$ 2-ciclo $\circ$ 2-ciclo $\circ$ 3-ciclo ou

    $\sigma =$ 4-ciclo $\circ$ 3-ciclo, nesses casos, σ tem ordem 12.

Portanto as únicas ordens possíveis para um elemento de S_7 são

$\underbrace{1, 2, 3, 4, 5, 6, 7}_{r\text{-ciclos}}$, $\underbrace{10 \text{ e } 12}_{\text{produto de ciclos}}$.

$\square$